UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/790,082	03/02/2004	Takeo Yoshida	118918	2490

25944 7590 09/19/2007

OLIFF & BERRIDGE, PLC
P.O. BOX 19928
ALEXANDRIA, VA 22320

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
09/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/790,082	YOSHIDA, TAKEO	
	Examiner	Art Unit	
	Oscar A. Louie	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 July 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-7 and 9-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-7 and 9-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This final action is in response to the amendment filed on 07/03/07. Claims 1-3, 5-7, & 9-13 are pending and have been considered as follows.

Examiner's Note

The examiner notes that the 35 U.S.C. 102(b) and 35 U.S.C. 103(a) rejections below are based on the current understanding of the current set of amended claims. Due to the nature of the current amended claim language, there are aspects which are difficult to understand clearly and definitely. The examiner has included a set of 35 U.S.C. 112 second paragraph rejections in order to point out the portions of the applicant's limitations which are indefinite and require clarification. It is also noted that the previous 35 U.S.C. 112 first paragraph rejection for Claim 10 has been withdrawn in light of the amendments.

Claim Objections

The applicant's amendments lack proper citation in their response as to the location of support in the applicant's specification disclosure for each amended claim. The applicant is required to disclose proof of support from their disclosure for their amendments in order to assure that no new matter has been added as a result of the amendments. The examiner notes that sufficient proof of support may be in the form of the Claim number, page, followed by the line number(s) where there is support for each amended claim limitation (i.e. "Support for Claim 1 may be found in the applicant's specification on page(s) 2-3 line(s) 45-60").

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1-3, 5-7, & 9-13 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The claims are generally narrative and indefinite, failing to conform with current U.S. practice. They appear to be a literal translation into English from a foreign document and are replete with grammatical and idiomatic errors.

The examiner notes that the applicant's amendments render the claim language to be generally difficult to interpret a clear and definite understanding of the invention for at least the following reasons below:

Regarding Claim 1:

- Page 2 lines 9-10 recite the limitation "associating the second connection authentication information with a connection server address of the connection server," which is indefinite as a result of the term "associating" which fails to clearly define the scope of "associating" authentication information with a server address.
- Page 2 lines 11-12 recite the limitation "a first unit for acquiring the second connection authentication information from the client apparatus" which is a contradiction with the earlier limitation which recites "second connection authentication information generated by the connection server."

- Page 2 lines 19-21 recite the limitation "a third unit for transmitting the second connection authentication information to the authentication server together with the connection request" which creates confusion as to the purpose of a unit of the authentication server transmitting information to itself.
- Page 3 lines 8-10 recite the limitation "a sixth unit for allowing the first connection authentication information to be received from the client address which is received from the authentication server" which creates confusion with whether the "first connection authentication information" is received from the client address or the authentication server. Additional confusion lies in whether it is the "first authentication information" or "the client address" which is received from the authentication server.

Regarding Claim 2:

- Claim 2 depends from Claim 1 and is rejected for being dependent on limitations that have been rejected for the reasons above as in Claim 1.

Regarding Claim 3:

- Page 4 lines 5-6 recite the limitation "a retention unit for associating each second connection authentication information with a connection server address of the corresponding connection server" which is indefinite as a result of the term "associating" which fails to clearly define the scope of "associating" authentication information with a server address.

Regarding Claim 5:

- Page 4 lines 12-15 recite the limitation "a control unit for receiving a client address of the client apparatus from the authentication server after the authentication server authenticates information received from the client address and allowing authentication information to be received from the client address" where lines 16-18 recites the limitation "an authentication unit for receiving the authentication information from the client apparatus having the client address to perform an authentication process by using the authentication information." These portions are confusing and unclear as it appears that both the connection server authentication unit and the authentication server receive the same authentication information from the client to perform an authentication process. That is, there appears to be a lack of corresponding part(s) which tie these limitations together to disclose the scope of the applicant's invention.

Regarding Claim 6:

- Page 4 lines 24-25 recite the limitation "a retention unit for storing a first encrypted user name and a first encrypted password, which are encrypted by a first encryption method" which is indefinite for being unclear as to whether the "first encrypted user name and first encrypted password" are a first set of user name and password and/or a set of user name and password encrypted by a first encryption method. It is also unclear as to whether there is a clear definition as to the difference between "a first encryption method" and "a second encryption method."

- Page 5 lines 1-2 recite the limitation "associating a connection server address of the connection server with the first encrypted user name and first encrypted password" which is indefinite as a result of the term "associating" which fails to clearly define the scope of "associating" authentication information with a server address.
- Page 5 lines 20-22 recite the limitation "generated by encrypting using a second encryption method a user name and a password input by the user" which is indefinite as being unclear as to which unit/component generates the "second encrypted user name and second encrypted password." It is also unclear as to whether the "input by the user" is the same set of input used for the "first encrypted user name and first encrypted password."

Regarding Claim 7:

- Page 6 lines 4-7 recite the limitations "a retention unit for storing user names and passwords, which are encrypted by a predetermined method" and "associating each user name and each password with a connection server address of a corresponding connection server" which are indefinite since it is unclear as to the scope of "a predetermined method" and "associating" a user name and password with a connection server address.

Regarding Claim 9:

- Pages 6-7 lines 23-25 & 1-4 recite the limitations "a connection request unit for transmitting to the authentication server a connection request and a user name and a password which are encrypted by a first encryption method" and "encrypting by a second

encryption method the user name and the password input by a user" which are indefinite as it is difficult to determine if the "first encryption method" and "second encryption method" are the same, as well as, the scope of their definition.

- Page 7 lines 5-9 recite the limitation "associating unique information of the client apparatus with at least one of a user name and a password previously provided to the connection server" which is indefinite as to the scope of "associating" client information with at least one of a user name and password. In addition, there is confusion as to the limitation made between the "unique information" and the user name and password when the user name and password were submitted to the local authentication unit for generating the unique information based on the user name and password. This would imply that the two are already "associated."

Regarding Claim 10:

- Page 8 lines 1-2 recite the limitation "a control unit that receives from the authentication server an address of the client apparatus and allows communication from the address of the client apparatus for a predetermined period" which is indefinite as to the definition of "a predetermined period."

Regarding Claim 11:

- Page 8 lines 11-17 recite the limitations "calculates first authentication information unique to the client apparatus to register the first authentication information in the connection server" and "acquires local authentication information from the connection server" and "the local authentication information associating the first authentication information with a predetermined authentication information and second authentication

information with the predetermined authentication information" and "stores the local authentication information" which are indefinite as it is difficult to determine what the "first authentication information unique to the client apparatus" is. It is also difficult to determine what the "local authentication information" consists of and where it came from. In addition, it is unclear what "associating" first/second authentication information with predetermined authentication information entails. "Predetermined authentication information" is also indefinite as to which authentication information it refers to, if any.

- Page 8-9 lines 18-25 & 1-2 recite the limitations "receives second authentication information input by a user when the user instructs a connection request with respect to the connection server" and "again calculates the first authentication information unique to the client apparatus" and "authenticates the second authentication information and the again calculated first authentication information based on the stored local authentication information" and "if authentication is successful, encrypts the second authentication information by a first encryption method" and "transmits the encrypted second authentication information to the authentication server" which are indefinite as it is appears that the second authentication information is input by a user and the first authentication information is calculated unique to the client, however, there is confusion as to the details of what "unique to the client" entails. It is also difficult to follow the logic for the portion which recites that authentication depends on the stored local authentication information for the second authentication information and first authentication information. That is, the location and interactions of all of the sets of authentication information are difficult to follow and track without there being confusion

as to which information is generated where, sent to which of the three apparatuses (e.g. client, authentication server, or connection server), and what information was used to create each set of authentication information in order to tie the applicant's intended purpose of invention all together clearly.

Regarding Claim 12:

- Page 9 lines 16-17 recite the limitation "associating the second connection authentication information with a connection server address of the connection server" which is indefinite as to the scope of the term "associating" which fails to clearly define the scope of "associating" authentication information with a server address.
- Page 9 lines 18-23 recites the limitations "transmitting by the client apparatus to the authentication server a second connection authentication information as user identification information together with a connection request" and "acquiring a client address and the user identifying information from the client apparatus when the authentication server receives the connection request from the client apparatus" which are indefinite as they do not clearly define what "user identification/identifying information" may consist of. The applicant appears to refer to "second authentication information" as being one form of "user identification/identifying information" which is generated based on"first authentication information." However, there is a lack of distinction between the "first" and "second" authentication information in this claim. That is, it is difficult to determine if the "first authentication information" is the same as the "second authentication information.

- Pages 9-10 lines 24-25 & 1-2 recite the limitation "transmitting the client address to the connection server address of the connection server when the user identification information is authenticated based on the second connection authentication information" which is indefinite as it creates confusion with performing authentication on the "user identification information" based on the "second authentication information" when the invention appears to primary deal with authenticating first, second, and local authentication information. It is also unclear as to which component of the invention performs the "acquiring."
- Page 10 lines 3-4 recite the limitation "transmitting by the client apparatus the connection server address from the authentication server" which is indefinite as it is unclear as to which component of the invention performs the "transmitting."

Regarding Claim 13:

- Page 10 lines 16-17 recite the limitation "storing by the authentication server a user name and a password which are encrypted by a first encryption method" which is indefinite as there is a lack of distinction between the first encryption method and the second encryption method. That is, it is difficult to determine if the two are the same method or two different methods of encryption.
- Page 10 lines 18-19 recite the limitation "associating the encrypted user name and the encrypted password with a connection server address of the connection server" which is indefinite as to the scope of "associating" encrypted user name and password with a server address. It is also difficult to determine which device/component of the applicant's invention performs the associating.

- Page 11 lines 1-3 recite the limitation "acquiring a client address of the client apparatus and the user name and the password, which are encrypted by the first encryption method, as information identifying a user of the client apparatus" which is indefinite as to which device/component of the applicant's invention performs the "acquiring."
- Page 11 lines 4-6 recite the limitation "transmitting the client address to the connection server address" which is indefinite as to which device/component of the applicant's invention performs the "transmitting."
- Page 11 line 9 recites the limitation "allowing communication from the client apparatus" which is indefinite as to which device/component of the applicant's invention performs the "allowing."
- Page 11 lines 10-11 recites the limitation "transmitting to the authentication server information indicating that the connection server has shifted to a connection wait state" which is indefinite as to which device/component of the applicant's invention performs the "transmitting."
- Page 11 lines 12-13 recites the limitation "encrypting using a second encryption method a user name and a password input by a user" which is indefinite as to which device/component of the applicant's invention performs the "encrypting."
- Page 11 lines 14-16 recites the limitation "transmitting to the connection server address the user name and the password which are encrypted by the second encryption method" which is indefinite as to which device/component of the applicant's invention performs the "transmitting."

It is noted by the examiner that throughout the claims, it is indefinite as to the definition of what a "first, second, third, etc units" may entail in light of the specification. It also appears that part of the confusion with the claim language is the result of the usage of the term "address" which adds confusion to the source and destination of information transmission since it is generally understood by one of ordinary skill in the art that communication networks involving multiple devices on a typical network (i.e. the Internet or an Ethernet network) would involve the sending of "addresses" between devices in order for the information to be properly routed from their source to their destination and vice versa. This is especially the case as it appears that the applicant's claims do not use the term "address" consistently throughout their claim language. Thus, drawing uncertainty as to whether the applicant is claiming specifics regarding the usage of address information and/or claiming address details in an attempt to clarify any confusion regarding the communication among devices/components of the applicant's invention. There is also the issue of the claim language being indefinite as to which device/component of the applicant's invention performs each particular process.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 5 & 10 are rejected under 35 U.S.C. 102(b) as being anticipated by Zhang et al. (US-6253327-B1).

Claim 5:

Zhang et al. disclose a connection server operating with an authentication server and a client apparatus comprising,

- "a control unit for receiving a client address of the client apparatus from the authentication server after the authentication server authenticates information received from the client address" (i.e. "at reference number 190, the authentication reply indicates that the authentication process was successful then, at reference number 200, the gateway device notifies the host by generating and sending an LCP access-accept packet from the gateway device to the host") [column 7 lines 20-25];
- "a control unit for allowing authentication information to be received from the client address" (i.e. "At reference number 150, the gateway device receives the LCP packets containing the authorization and authentication information from the host computer") [column 7 lines 8-10];

- "an authentication unit for receiving the authentication information from the client apparatus having the client address to perform an authentication process by using the authentication information" (i.e. "the authentication server sends an authentication reply back to the gateway device that confirms the status of the authentication") [column 7 lines 18-20].

Claim 10:

Zhang et al. disclose a connection server operating with a client apparatus and an authentication server comprising,

- "a control unit that receives from the authentication server an address of the client apparatus and allows communication from the address of the client apparatus for a predetermined period" (i.e. "If, at reference number 190, the authentication reply indicates that the authentication process was successful then, at reference number 200, the gateway device notifies the host by generating and sending an LCP access-accept packet from the gateway device to the host") [column 7 lines 20-25];
- "a transmitting unit that transmits to the authentication server information indicating that the connection server has shifted to a connection wait state" (i.e. "If the authentication reply indicates that the authentication process was unsuccessful then, at reference number 210, the gateway device sends a prompt back to the host notifying the subscriber that the authentication process was unsuccessful") [column 7 lines 25-29].

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 3, & 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zhang et al. (US-6253327-B1).

Claim 1:

Zhang et al. disclose a network connection system comprising,

- "a client apparatus" (i.e. "the host computer") [column 7 line 10];
- "a third unit for transmitting the second connection authentication information to the authentication server together with the connection request" (i.e. "At reference number 150, the gateway device receives the LCP packets containing the authorization and authentication information from the host computer") [column 7 lines 8-10];
- "a fifth unit for preparing the first connection authentication information based on the user identification information" (i.e. "At reference number 150, the gateway device receives the LCP packets containing the authorization and authentication information from the host computer") [column 7 lines 8-10];
- "a fifth unit for transmitting the first connection authentication information to the connection server address of the connection server" (i.e. "At reference number 150, the gateway device receives the LCP packets containing the authorization and authentication information from the host computer") [column 7 lines 8-10];

- "an authentication server" (i.e. "an authentication server") [column 7 lines 11-12];
- "a retention unit for storing second connection authentication information generated by the connection server based on user identification information" (i.e. "The user profiles are stored within the memory of the authentication server or a local cache in communication with the authentication server") [column 7 lines 15-17];
- "a retention unit for associating the second connection authentication information with a connection server address of the connection server" (i.e. "The user profiles are stored within the memory of the authentication server or a local cache in communication with the authentication server") [column 7 lines 15-17];
- "a first unit for acquiring the second connection authentication information from the client apparatus and a client address of the client apparatus when the first unit receives a connection request from the client apparatus" (i.e. "the gateway device receives the LCP packets containing the authorization and authentication information from the host computer") [column 7 lines 8-10];
- "a second unit for transmitting the client address to the connection server address associated with the second connection authentication information acquired by the first unit" (i.e. "The gateway device, at reference number 160, generates and forwards to an authentication server") [column 7 lines 10-12];
- "a connection server" (i.e. "the gateway device") [column 7 line 8];

- "a sixth unit for allowing the first connection authentication information to be received from the client address which is received from the authentication server" (i.e. "column 7 lines 18-20at reference number 180, the authentication server sends an authentication reply back to the gateway device that confirms the status of the authentication") [column 7 lines 18-20];
- "a seventh unit for performing an authentication process by using the first connection authentication information transmitted from the client address" (i.e. "The gateway device, at reference number 160, generates and forwards to an authentication server a RADIUS account logon request packet") [column 7 lines 10-12];

but they do not explicitly disclose,

- "a fourth unit for receiving the connection server address from the authentication server"
- "a second unit for transmitting the connection server address to the client apparatus"

however, Zhang et al. do disclose,

- "the gateway device notifies the host by generating and sending an LCP access-accept packet from the gateway device to the host" [column 7 lines 23-25];
- "the authentication server sends an authentication reply back to the gateway device that confirms the status of the authentication" [column 7 lines 18-20];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a fourth unit for receiving the connection server address from the authentication server" and "a second unit for transmitting the connection server address to the

client apparatus," in the invention as disclosed by Zhang et al. since it is implied that the address of each communicating device would have to be sent with response messages in order to identify the sender.

Claim 3:

Zhang et al. disclose an authentication server for being connected to a plurality of client apparatuses and a plurality of connection servers comprising,

- "a retention unit for storing second connection authentication information generated based on user identification information" (i.e. "The user profiles are stored within the memory of the authentication server or a local cache in communication with the authentication server") [column 7 lines 15-17];
- "a retention unit for associating each second connection authentication information with a connection server address of the corresponding connection server" (i.e. "The user profiles are stored within the memory of the authentication server or a local cache in communication with the authentication server") [column 7 lines 15-17];
- "a first unit for acquiring the second connection authentication information from the client apparatus and a client address when the first unit receives a connection request from the client apparatus" (i.e. "the gateway device receives the LCP packets containing the authorization and authentication information from the host computer") [column 7 lines 8-10];

- "a second unit for transmitting the acquired client address to the connection server address of the connection server associated with the acquired second connection authentication information" (i.e. "The gateway device, at reference number 160, generates and forwards to an authentication server") [column 7 lines 10-12];

but they do not explicitly disclose,

- "a second unit for transmitting the connection server address to the client apparatus which has transmitted the connection request"

however, Zhang et al. do disclose,

- "the authentication server sends an authentication reply back to the gateway device that confirms the status of the authentication" [column 7 lines 18-20];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a second unit for transmitting the connection server address to the client apparatus which has transmitted the connection request," in the invention as disclosed by Zhang et al. since it is implied that the address of each communicating device would have to be sent with response messages in order to identify the sender.

Claim 12:

Zhang et al. disclose a connection method using a network connection system including a client apparatus, an authentication server, and a connection server comprising,

- "storing in the authentication server second connection authentication information generated by the connection server based on first connection authentication information" (i.e. "The user profiles are stored within the memory of the authentication server or a local cache in communication with the authentication server") [column 7 lines 15-17];

- "associating the second connection authentication information with a connection server address of the connection server" (i.e. "The user profiles are stored within the memory of the authentication server or a local cache in communication with the authentication server") [column 7 lines 15-17];
- "transmitting by the client apparatus to the authentication server a second connection authentication information as user identification information together with a connection request" (i.e. "At reference number 150, the gateway device receives the LCP packets containing the authorization and authentication information from the host computer") [column 7 lines 8-10];
- "acquiring a client address and the user identifying information from the client apparatus when the authentication server receives the connection request from the client apparatus" (i.e. "At reference number 150, the gateway device receives the LCP packets containing the authorization and authentication information from the host computer") [column 7 lines 8-10];
- "transmitting the client address to the connection server address of the connection server when the user identification information is authenticated based on the second connection authentication information" (i.e. "The user profiles are stored within the memory of the authentication server or a local cache in communication with the authentication server") [column 7 lines 18-20];

- "transmitting by the client apparatus a first connection authentication information to the connection server address" (i.e. "At reference number 150, the gateway device receives the LCP packets containing the authorization and authentication information from the host computer") [column 7 lines 8-10];
- "receiving by the connection server the first connection authentication information from the client address" (i.e. "At reference number 150, the gateway device receives the LCP packets containing the authorization and authentication information from the host computer") [column 7 lines 8-10];
- "performing an authentication process by using the first connection authentication information transmitted from the client address" (i.e. "The gateway device, at reference number 160, generates and forwards to an authentication server") [column 7 lines 10-12];

but they do not explicitly disclose,

- "transmitting by the client apparatus the connection server address from the authentication server"
- "receiving by the client apparatus the connection server address from the authentication server"

however, Zhang et al. do disclose,

- "the gateway device notifies the host by generating and sending an LCP access-accept packet from the gateway device to the host" [column 7 lines 23-25];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "transmitting by the client apparatus the connection server address from the authentication server" and "receiving by the client apparatus the connection server address from the authentication server," in the invention as disclosed by Zhang et al. since it is implied that the address of each communicating device would have to be sent with response messages in order to identify the sender.

7. Claims 2, 6, 7, 9, 11, & 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zhang et al. (US-6253327-B1) in view of Leveridge et al. (US-7233997-B1).

Claim 2:

Zhang et al. disclose a network connection system, as in Claim 1 above, but do not disclose,

- "the second connection authentication information is a message digest of the first connection authentication information"

however, Leveridge et al. do disclose,

- "On the client side, the username and password are input by the user into the terminal, and the SPC combines the two and performs the hash function H0 to produce a first hash. The first hash is combined with the challenge received by the SPC from the SPS and input to a second hash function H1 to produce a second hash" [column 5 lines 29-34];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the second connection authentication information is a message digest of the first connection authentication information," in the invention as disclosed by

Zhang et al. for the purposes of "given M, it is extremely difficult to compute or find another message, M' such that H(M')=h" [column 5 lines 26-27]. Thus, improving the difficulty of decrypting the message (i.e. authentication information) by an unauthorized party.

Claim 6:

Zhang et al. disclose a network connection system comprising,

- "a client apparatus" (i.e. "the host computer") [column 7 line 10];
- "an authentication server" (i.e. "an authentication server") [column 7 lines 11-12];
- "a retention unit for storing a first encrypted user name and a first encrypted password, which are encrypted by a first encryption method" (i.e. "The user profiles are stored within the memory of the authentication server or a local cache in communication with the authentication server") [column 7 lines 15-17];
- "a retention unit for associating a connection server address of the connection server with the first encrypted user name and first encrypted password" (i.e. "The user profiles are stored within the memory of the authentication server or a local cache in communication with the authentication server") [column 7 lines 15-17];
- "a first unit for acquiring the first encrypted user name and the first encrypted password" (i.e. "At reference number 150, the gateway device receives the LCP packets containing the authorization and authentication information from the host computer") [column 7 lines 8-10];

- "a first unit for acquiring a client address when the first unit receives a connection request from the client apparatus" (i.e. "At reference number 150, the gateway device receives the LCP packets containing the authorization and authentication information from the host computer") [column 7 lines 8-10];
- "a second unit for receiving from the connection server information indicating that the connection server has shifted to a connection wait state" (i.e. "The gateway device, at reference number 160, generates and forwards to an authentication server") [column 7 lines 10-12];
- "a second unit for transmitting the acquired client address to the connection server address associated with the user identification information" (i.e. "If the authentication reply indicates that the authentication process was unsuccessful then, at reference number 210, the gateway device sends a prompt back to the host notifying the subscriber that the authentication process was unsuccessful") [column 7 lines 25-29];
- "a connection server" (i.e. "the gateway device") [column 7 line 8];

but they do not explicitly disclose,

- "a fourth unit for receiving the connection server address from the authentication server"
- "a second unit for transmitting the connection server address to the client apparatus"

and they do not disclose,

- "a third unit for transmitting to the authentication server the first encrypted user name and the first encrypted password, which are encrypted by the first encryption method together with the connection request"

- "a fourth unit for transmitting to the connection server address a second encrypted user name and a second encrypted password, which are generated by encrypting using a second encryption method a user name and a password input by the user"
- "the first encrypted user name and the first encrypted password being an identification for identifying a user of the client apparatus"

however, Zhang et al. do disclose,

- "the gateway device notifies the host by generating and sending an LCP access-accept packet from the gateway device to the host" [column 7 lines 23-25];
- "the authentication server sends an authentication reply back to the gateway device that confirms the status of the authentication" [column 7 lines 18-20];

and Leveridge et al. do disclose,

- "On the client side, the username and password are input by the user into the terminal, and the SPC combines the two and performs the hash function H0 to produce a first hash. The first hash is combined with the challenge received by the SPC from the SPS and input to a second hash function H1 to produce a second hash" [column 5 lines 29-34];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a fourth unit for receiving the connection server address from the authentication server" and "a second unit for transmitting the connection server address to the client apparatus" and "a third unit for transmitting to the authentication server the first encrypted user name and the first encrypted password, which are encrypted by the first encryption method together with the connection request" and "a fourth unit for transmitting to the connection server address a second encrypted user name and a second encrypted password, which are generated by

encrypting using a second encryption method a user name and a password input by the user" and "the first encrypted user name and the first encrypted password being an identification for identifying a user of the client apparatus," in the invention as disclosed by Zhang et al. since it is implied that the address of each communicating device would have to be sent with response messages in order to identify the sender. In addition, the use of nested encryption/hashing would be for the purposes of "given M, it is extremely difficult to compute or find another message, M' such that H(M')=h" [column 5 lines 26-27]. Thus, improving the difficulty of decrypting the message (i.e. authentication information) by an unauthorized party.

Claim 7:

Zhang et al. disclose an authentication server operating with a plurality of client apparatuses and a plurality of connection servers comprising,

- "a first unit for acquiring an acquired encrypted user name, an acquired encrypted password, and an acquired client address when the first unit receives a connection request from the client apparatus" (i.e. "At reference number 150, the gateway device receives the LCP packets containing the authorization and authentication information from the host computer") [column 7 lines 8-10];
- "a second unit for transmitting the acquired client address to the connection server address associated with the acquired encrypted user name and password" (i.e. "The gateway device, at reference number 160, generates and forwards to an authentication server") [column 7 lines 10-12];

- "a second unit for receiving from the connection server information indicating that the connection server has shifted to a connection wait state" (i.e. "If the authentication reply indicates that the authentication process was unsuccessful then, at reference number 210, the gateway device sends a prompt back to the host notifying the subscriber that the authentication process was unsuccessful") [column 7 lines 25-29];

but they do not explicitly disclose,

- "a second unit for transmitting the connection server address to the client apparatus, which has issued the connection request"

and they do not disclose,

- "a third unit for transmitting to the authentication server the first encrypted user name and the first encrypted password, which are encrypted by the first encryption method together with the connection request"
- "a fourth unit for transmitting to the connection server address a second encrypted user name and a second encrypted password, which are generated by encrypting using a second encryption method a user name and a password input by the user"
- "the first encrypted user name and the first encrypted password being an identification for identifying a user of the client apparatus"

however, Zhang et al. do disclose,

- "the authentication server sends an authentication reply back to the gateway device that confirms the status of the authentication" [column 7 lines 18-20];

and Leveridge et al. do disclose,

- "On the client side, the username and password are input by the user into the terminal, and the SPC combines the two and performs the hash function H0 to produce a first hash. The first hash is combined with the challenge received by the SPC from the SPS and input to a second hash function H1 to produce a second hash" [column 5 lines 29-34];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the authentication server sends an authentication reply back to the gateway device that confirms the status of the authentication" and "a retention unit for storing user names and passwords, which are encrypted by a predetermined method" and "a retention unit for associating each user name and each password with a connection server address of a corresponding connection server" and "the encrypted user name and password being an identification information of a user of the client apparatus," in the invention as disclosed by Zhang et al. since it is implied that the address of each communicating device would have to be sent with response messages in order to identify the sender. In addition, the use of nested encryption/hashing would be for the purposes of "given M, it is extremely difficult to compute or find another message, M' such that H(M')=h" [column 5 lines 26-27]. Thus, improving the difficulty of decrypting the message (i.e. authentication information) by an unauthorized party.

Claim 9:

Zhang et al. disclose a client apparatus operating with an authentication server and a connection server comprising,

- "a connection request unit for transmitting to the authentication server a connection request and a user name and a password which are encrypted by a first encryption method" (i.e. "the host computer") [column 7 line 10];
- "the connection request unit transmits to the authentication server the connection request and the user name and the password which are encrypted by the first method only when the user name and the password input by the user are authenticated by the local authentication unit" (i.e. "At reference number 150, the gateway device receives the LCP packets containing the authorization and authentication information from the host computer") [column 7 lines 8-10];
- "a transmitting unit for transmitting the encrypted user name and password to the connection server address" (i.e. "The gateway device, at reference number 160, generates and forwards to an authentication server") [column 7 lines 10-12];
- "a retention unit for storing local authentication information, which is previously supplied from the connection server" (i.e. "The user profiles are stored within the memory of the authentication server or a local cache in communication with the authentication server") [column 7 lines 15-17];

but they do not explicitly disclose,

- "a receiving unit for receiving a connection server address from the authentication server"

and they do not disclose,

- "encrypting by a second encryption method the user name and the password input by a user"
- "the local authentication information associating unique information of the client apparatus with at least one of a user name and a password previously provided to the connection server"
- "a local authentication unit for generating the unique information based on a user name and the password input by the user"
- "a local authentication unit for authenticating the user name and the password input by the user by judging based on the local authentication information whether or not at least one of the user name and the password input by the user is associated with the unique information"

however, Zhang et al. do disclose,

- "the gateway device notifies the host by generating and sending an LCP access-accept packet from the gateway device to the host" [column 7 lines 23-25];

and Leveridge et al. do disclose,

- "On the client side, the username and password are input by the user into the terminal, and the SPC combines the two and performs the hash function H0 to produce a first hash. The first hash is combined with the challenge received by the SPC from the SPS and input to a second hash function H1 to produce a second hash" [column 5 lines 29-34];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a receiving unit for receiving a connection server address from the authentication server " and "encrypting by a second encryption method the user name and the password input by a user" and "the local authentication information associating unique information of the client apparatus with at least one of a user name and a password previously provided to the connection server" and "a local authentication unit for generating the unique information based on a user name and the password input by the user" and "a local authentication unit for authenticating the user name and the password input by the user by judging based on the local authentication information whether or not at least one of the user name and the password input by the user is associated with the unique information," in the invention as disclosed by Zhang et al. since it is implied that the address of each communicating device would have to be sent with response messages in order to identify the sender. In addition, the use of nested encryption/hashing would be for the purposes of "given M, it is extremely difficult to compute or find another message, M' such that H(M')=h" [column 5 lines 26-27]. Thus, improving the difficulty of decrypting the message (i.e. authentication information) by an unauthorized party.

Claim 11:

Zhang et al. disclose a network connection system comprising,

- "a client apparatus" (i.e. "the host computer") [column 7 line 10];
- "acquires local authentication information from the connection server" (i.e. "At reference number 150, the gateway device receives the LCP packets containing the authorization and authentication information from the host computer") [column 7 lines 8-10];

- "the local authentication information associating the first authentication information with a predetermined authentication information and second authentication information with the predetermined authentication information" (i.e. "The user profiles are stored within the memory of the authentication server or a local cache in communication with the authentication server") [column 7 lines 15-17];
- "stores the local authentication information" (i.e. "The user profiles are stored within the memory of the authentication server or a local cache in communication with the authentication server") [column 7 lines 15-17];
- "receives second authentication information input by a user when the user instructs a connection request with respect to the connection server" (i.e. "At reference number 150, the gateway device receives the LCP packets containing the authorization and authentication information from the host computer") [column 7 lines 8-10];
- "transmits the encrypted second authentication information to the authentication server" (i.e. "At reference number 150, the gateway device receives the LCP packets containing the authorization and authentication information from the host computer") [column 7 lines 8-10];
- "transmits to the connection server address the second authentication information encrypted by a second encryption method" (i.e. "At reference number 150, the gateway device receives the LCP packets containing the authorization and authentication information from the host computer") [column 7 lines 8-10];

- "starts a communication with the connection server" (i.e. "At reference number 150, the gateway device receives the LCP packets containing the authorization and authentication information from the host computer") [column 7 lines 8-10];
- "an authentication server for supplying information guiding a connection destination to the client apparatus" (i.e. "an authentication server") [column 7 lines 11-12];
- "a connection server" (i.e. "the gateway device") [column 7 line 8];

but they do not explicitly disclose,

- "receives from the authentication server a connection server address of the connection server"

and they do not disclose,

- "calculates first authentication information unique to the client apparatus to register the first authentication information in the connection server"
- "again calculates the first authentication information unique to the client apparatus"
- "authenticates the second authentication information and the again calculated first authentication information based on the stored local authentication information"
- "if authentication is successful, encrypts the second authentication information by a first encryption method"

however, Zhang et al. do disclose,

- "the authentication server sends an authentication reply back to the gateway device that confirms the status of the authentication" [column 7 lines 18-20];

and Leveridge et al. do disclose,

- "On the client side, the username and password are input by the user into the terminal, and the SPC combines the two and performs the hash function H0 to produce a first hash. The first hash is combined with the challenge received by the SPC from the SPS and input to a second hash function H1 to produce a second hash" [column 5 lines 29-34];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "receives from the authentication server a connection server address of the connection server" and "calculates first authentication information unique to the client apparatus to register the first authentication information in the connection server" and "again calculates the first authentication information unique to the client apparatus" and "authenticates the second authentication information and the again calculated first authentication information based on the stored local authentication information" and "if authentication is successful, encrypts the second authentication information by a first encryption method," in the invention as disclosed by Zhang et al. since it is implied that the address of each communicating device would have to be sent with response messages in order to identify the sender. In addition, the use of nested encryption/hashing would be for the purposes of "given M, it is extremely difficult to compute or find another message, M' such that H(M')=h" [column 5 lines 26-27]. Thus, improving the difficulty of decrypting the message (i.e. authentication information) by an unauthorized party.

Claim 13:

Zhang et al. disclose a connection method using a network connection system including a client apparatus, an authentication server, and a connection server comprising,

- "storing by the authentication server a user name and a password which are encrypted by a first encryption method" (i.e. "The user profiles are stored within the memory of the authentication server or a local cache in communication with the authentication server") [column 7 lines 15-17];
- "associating the encrypted user name and the encrypted password with a connection server address of the connection server" (i.e. "The user profiles are stored within the memory of the authentication server or a local cache in communication with the authentication server") [column 7 lines 15-17];
- "transmitting by the client apparatus to the authentication server a connection request and the user name and the password which are encrypted by the first encryption method" (i.e. "At reference number 150, the gateway device receives the LCP packets containing the authorization and authentication information from the host computer") [column 7 lines 8-10];
- "receiving by the authentication server the connection request from the client apparatus" (i.e. "At reference number 150, the gateway device receives the LCP packets containing the authorization and authentication information from the host computer") [column 7 lines 8-10];

- "acquiring a client address of the client apparatus and the user name and the password, which are encrypted by the first encryption method, as information identifying a user of the client apparatus" (i.e. "At reference number 150, the gateway device receives the LCP packets containing the authorization and authentication information from the host computer") [column 7 lines 8-10];
- "transmitting the client address to the connection server address" (i.e. "the authentication server sends an authentication reply back to the gateway device that confirms the status of the authentication") [column 7 lines 18-20];
- "receiving by the connection server the client address" (i.e. "At reference number 150, the gateway device receives the LCP packets containing the authorization and authentication information from the host computer") [column 7 lines 8-10];
- "allowing communication from the client apparatus" (i.e. "the authentication server sends an authentication reply back to the gateway device that confirms the status of the authentication") [column 7 lines 18-20];
- "transmitting to the authentication server information indicating that the connection server has shifted to a connection wait state" (i.e. "If the authentication reply indicates that the authentication process was unsuccessful then, at reference number 210, the gateway device sends a prompt back to the host notifying the subscriber that the authentication process was unsuccessful") [column 7 lines 25-29];

and they do not disclose,

- "encrypting using a second encryption method a user name and a password input by a user"

- "transmitting to the connection server address the user name and the password which are encrypted by the second encryption method"
- "performing an authentication process by using the user name and the password which are encrypted by the second encryption method and are received by the connection server from the client apparatus"

however, Leveridge et al. do disclose,

- "On the client side, the username and password are input by the user into the terminal, and the SPC combines the two and performs the hash function H0 to produce a first hash. The first hash is combined with the challenge received by the SPC from the SPS and input to a second hash function H1 to produce a second hash" [column 5 lines 29-34];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "encrypting using a second encryption method a user name and a password input by a user" and "transmitting to the connection server address the user name and the password which are encrypted by the second encryption method" and "performing an authentication process by using the user name and the password which are encrypted by the second encryption method and are received by the connection server from the client apparatus," in the invention as disclosed by Zhang et al. since it is implied that the address of each communicating device would have to be sent with response messages in order to identify the sender. In addition, the use of nested encryption/hashing would be for the purposes of "given M, it is extremely difficult to compute or find another message, M' such that H(M')=h" [column 5 lines 26-27]. Thus, improving the difficulty of decrypting the message (i.e. authentication information) by an unauthorized party.

Conclusion

8. Applicant's arguments with respect to claims 1-3, 5-7, & 9-13 have been considered but are moot in view of the new ground(s) of rejection as necessitated by the applicant's amendments.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
09/14/2007

Nasser Moazzami
Supervisory Patent Examiner